BlueKeep : Microsoft veut éviter un autre WannaCry

Si ce n'est déjà fait, patchez sans plus attendre la faille BlueKeep.

Microsoft fait passer le message après la découverte d'une série d'attaques exploitant cette vulnérabilité.

Immatriculée CVE-2019-0708, elle touche le protocole RDP (Remote Desktop Services) sur Windows 7 et Windows Server 2008 / 2008 R2.
La mise à disposition du correctif remonte au 14 mai dernier.

> *While we currently see only coin miners being dropped, we agree w/ the research community that CVE-2019-0708 (BlueKeep) exploitation can be big. Locate and patch exposed RDP services now. Read our latest blog w/ assist from @GossiTheDog & @MalwareTechBlog https://t.co/y1NgN5WVu8*
>
> *— Microsoft Security Intelligence (@MsftSecIntel) November 7, 2019*

La série d'attaques en question est probablement toujours en cours.
Microsoft a commencé à communiquer à son sujet des suites d'une alerte émise la semaine passée par un chercheur en sécurité.

> *CVE-2019-0708 RDP vulnerability megathread, aka BlueKeep.*
>
> *Going to nickname it BlueKeep as it's about as secure as the Red Keep in Game of Thrones, and often leads to a blue screen of death when exploited.*
>
> *— Kevin Beaumont (@GossiTheDog) 14 mai 2019*

Celui-ci avait mis en place des « pots de miel » spécifiquement conçus pour attirer les attaques fondées sur BlueKeep. Ils exposaient uniquement leur port 3389, réservé à l'assistance à distance sur RDP). Pour la première fois en quasiment six mois de fonctionnement, ils ont presque tous commencé à crasher régulièrement à partir du 23 octobre.

L'analyse des *dumps* a permis de détecter une tentative d'exploitation massive de BlueKeep pour diffuser un mineur de cryptomonnaie (Monero).

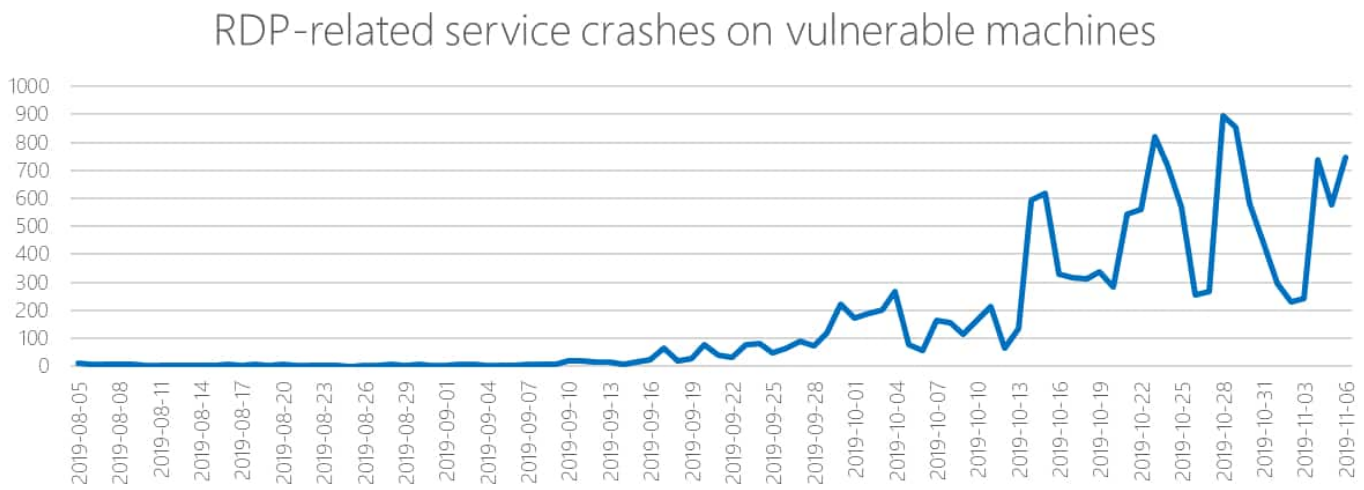
La piste Metasploit

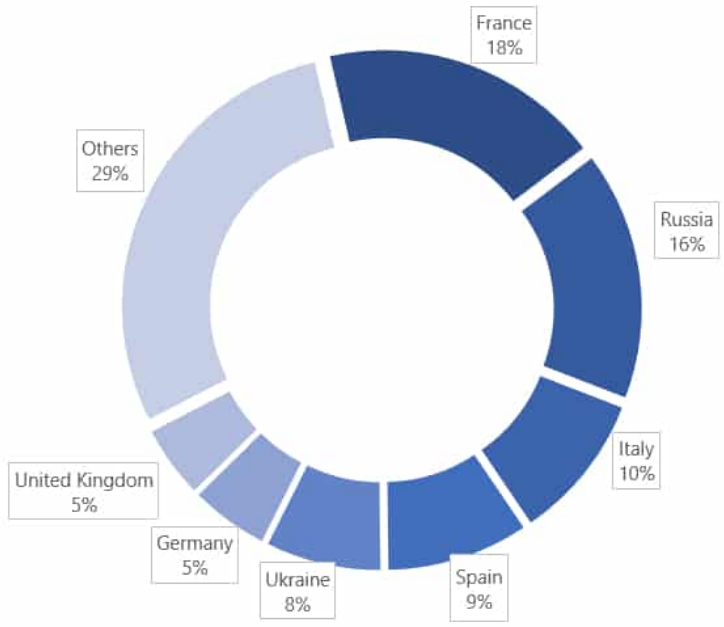
On avait déjà trouvé trace, en juillet, d'une offensive associant un détecteur de vulnérabilités BlueKeep et un cryptomineur. Il s'agissait d'une variante du *malware* Watchbog, qui visait à l'origine les serveurs Linux et s'était étendu aux systèmes Windows.

L'attaque qui a déclenché la communication de Microsoft ne semble pas liée à Watchbog. Elle se rapproche, en revanche, d'une autre campagne de diffusion de cryptomineurs repérée en septembre.

Elle utilise, d'une part, le même serveur de commande et de contrôle. Et de l'autre, le même vecteur d'exploitation de BlueKeep : un module intégré le 6 septembre à l'outil open source de test d'intrusion Metasploit.

Microsoft affirme avoir observé, sur « certains échantillons de machines vulnérables », une nette augmentation des attaques RDP depuis cette date.





La France fait partie des pays touchés (18 % des systèmes sur lesquels le cryptomineur a été retrouvé).

Le problème, d'après Microsoft, ne réside pas tant dans la forme actuelle de l'attaque que dans les *malware* qu'elle pourrait véhiculer à l'avenir.

Photo d'illustration © pzAxe – Shutterstock.com